- 2 -

IN THE CLAIMS

Amended claims follow:

1.      (Currently Amended) A method for verifying trusted status of a service-providing server in a peer-to-peer network, comprising:

broadcasting a request over the network by a requesting peer for a task with respect to a remote non-local backend server;

receiving a response to the request from the service-providing server;

verifying a digital certificate of the response issued by the remote non-local backend server indicating that the responding service-providing server is trusted for the requested task;

forwarding the task to a local alias URL of the responding peer for performance of the task by the responding server if said verifying is successful; and

awaiting for another response from another service-providing server if the verifying is unsuccessful;

wherein said verifying verifies that the local alias URL is approved by the non-local backend server for the requested task;

wherein a message is broadcasted indicating that the requesting peer has located the responding service-providing server;

wherein the local alias URL points to a local upload directory for a HTTP service server residing at a responding server node;

wherein the request specifies a post method that places data into the local upload directory as a uniquely named file.


2.      (Original) A method for verifying trusted status of a service-providing peer of claim 1, wherein the digital certificate is a 1024-bit VeriSign digital certificate.


3.      (Cancelled)

4.      (Original) A method for verifying trusted status of a service-providing peer of claim 1, further comprising placing the responding server node in a black list of the requesting peer for the requested task if said verifying is unsuccessful.

5.      (Cancelled)

6.      (Cancelled)

7.      (Cancelled)

8.      (Cancelled)

9.      (Currently Amended) A method for verifying trusted status of a service-providing peer of claim 1, wherein the task is an uploading task and wherein said forwarding the task to the local alias URL includes forwarding [a]the file to be uploaded to the remote non-local backend server.

10.     (Currently Amended) A computer program product for verifying trusted status of a service-providing peer in a peer-to-peer network, comprising:

computer code that broadcasts a request over the network by a requesting peer for a task with respect to a remote non-local backend server;

computer code that receives a response to the request from the service-providing server;

computer code that verifies a digital certificate of the response issued by the remote non-local backend server indicating that the responding service-providing server is trusted for the requested task;

computer code that forwards the task to a local alias URL of the responding peer for performance of the task by the responding server if said verifying is successful; and

computer code that awaits for another response from another service-providing server if the verifying is unsuccessful; and

a computer readable medium that stores said computer codes;

- 4 -

wherein said verifying verifies that the local alias URL is approved by the non-local backend server for the requested task;

wherein a message is broadcasted indicating that the requesting peer has located the responding service-providing server;

wherein the local alias URL points to a local upload directory for a HTTP service server residing at a responding server node;

wherein the request specifies a post method that places data into the local upload directory as a uniquely named file.

11.     (Original) A computer program product for verifying trusted status of a service providing peer of claim 10, wherein the digital certificate is a 1024-bit VeriSign digital certificate.

12.     (Cancelled)

13.     (Original) A computer program product for verifying trusted status of a service-providing peer of claim 10, further comprising computer code that places the responding server node in a black list of the requesting peer for the requested task if said verifying is unsuccessful.

14.     (Cancelled)

15.     (Cancelled)

16.     (Cancelled)

17.     (Cancelled)

18.     (Currently Amended) A computer program product for verifying trusted status of a service-providing peer of claim 10, wherein the task is an uploading task and

- 5 -

wherein computer code that forwards the task to the local alias URL includes computer code that forwards [a]the file to be uploaded to the remote non-local backend server.

19.     (New) A system for verifying trusted status of a service-providing server in a peer-to-peer network, comprising:

    means for broadcasting a request over the network by a requesting peer for a task with respect to a remote non-local backend server;

    means for receiving a response to the request from the service-providing server;

    means for verifying a digital certificate of the response issued by the remote non-local backend server indicating that the responding service-providing server is trusted for the requested task;

    means for forwarding the task to a local alias URL of the responding peer for performance of the task by the responding server if said verifying is successful; and

    means for awaiting for another response from another service-providing server if the verifying is unsuccessful;

    wherein said verifying verifies that the local alias URL is approved by the non-local backend server for the requested task;

    wherein a message is broadcasted indicating that the requesting peer has located the responding service-providing server;

    wherein the local alias URL points to a local upload directory for a HTTP service server residing at a responding server node;

    wherein the request specifies a post method that places data into the local upload directory as a uniquely named file.

20.     (New) A system for verifying trusted status of a service-providing peer of claim 19, wherein the digital certificate is a 1024-bit VeriSign digital certificate.

21.     (New) A system for verifying trusted status of a service-providing peer of claim 19, further comprising means for placing the responding server node in a black list of the requesting peer for the requested task if said verifying is unsuccessful.